Claims

What is claimed is:

1. A method for providing access to a secure entity or service by M designated persons having only limited access privileges comprising the steps of:

storing biometric data in dependence upon a biometric characteristic of each of the M designated persons;

capturing biometric information representative of a biometric characteristic of each of N persons and providing biometric data in dependence thereupon, with $1 < N < M$ being a subset of the M designated persons;

comparing the captured biometric data of each of the N persons with the stored biometric data to produce N comparison results; and,

if the N comparison results are indicative of the N persons each being one of the M designated persons and thereby forming a subset, determining access privileges to the secure entity or service in dependence upon the subset.

2. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 1, wherein the subset is any set of X designated persons, N being a predetermined number and X being greater than or equal to N.

3. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 1, wherein the subset is one of a plurality of predetermined subsets of N designated persons.

4. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 3, wherein each of the plurality of subsets comprises a different combination of persons of the M designated persons.

5. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 4, wherein different subsets comprise a different number of persons combined in the subset.

6. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 5, wherein the subsets of the plurality of subsets have different access privileges to the secure entity or service.

7. A method for providing access to a secure entity or service by M designated persons having only limited access privileges comprising the steps of:

providing each designated person of the M designated persons with a portable biometric device operable to capture biometric information presented thereto;

assigning a biometric characteristic of each of the M designated persons to a respective portable biometric device and storing biometric data in the respective portable biometric device in dependence upon the biometric characteristic;

capturing biometric information representative of a biometric characteristic of each of N persons in response to each of the N persons presenting said information to the respective portable biometric device and providing biometric data in dependence thereupon, with $1 < N < M$ being a subset of the M designated persons;

comparing the captured biometric data with biometric data stored in each of the respective portable biometric devices to produce a comparison result and, in dependence thereon performing one of transmitting an authorization signal from said portable biometric device to a receiving port of the secure entity or service and other than transmitting an authorization signal from said portable biometric device; and,

determining access privileges to the secure entity or service in dependence upon the authorization signals received from the respective portable biometric devices of the subset of N persons.

8. A method for providing access to a secure entity or service by a designated person having only limited access privileges as defined in claim 7, comprising the step of:

denying access to the secure entity or service in absence of at least N of M authorization signals.

9. A method for providing access to a secure entity or service by a designated person having only limited access privileges as defined in claim 7, wherein the subset of N persons comprises at least two persons of the M designated persons.

10. A method for providing access to a secure entity or service by M designated persons having only limited access privileges comprising the steps of:

storing biometric data in dependence upon a biometric characteristic of each of the M designated persons in at least a portable biometric device;

capturing biometric information representative of a biometric characteristic of each of N persons in response to each of the N persons presenting said information to one of the at least a portable biometric device and providing biometric data in dependence thereupon, with 1 < N < M being a subset of the M designated persons;

comparing the captured biometric data of each of the N persons with the stored biometric data to produce N comparison results;

if each of X comparison results is indicative of one of the N persons being one of the M designated persons, transmitting an authorization signal from the at least a portable biometric device to a receiving port of the secure entity or service, wherein 1 < X ≤ N; and,

determining access privileges to the secure entity or service in dependence upon the authorization signals of the subset of X persons received from the at least a portable biometric device.

11. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 10, wherein the determined access privileges define a time limitation.

12. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 10, wherein the determined access

privileges define functional limitations of the secure entity or service in dependence upon the subset of X persons.

13. A method for providing access to a secure entity or service by M designated persons having only limited access privileges as defined in claim 10, wherein X = N.

14. A security system for securing an entity or a service from indiscriminate access and for providing access to a subset of N persons of M designated persons comprising:
at least a portable biometric device, the device comprising:

a biometric sensor for capturing biometric information representative of a biometric characteristic in response to a person presenting said information to the biometric sensor;

an encoder for digitally encoding the captured biometric information and providing biometric data in dependence thereupon;

memory for storing biometric data of at least one of the M designated persons;

a processor for comparing the captured biometric data with stored biometric data of a designated person to produce a comparison result, and if the comparison result is indicative of a match for providing an authorization signal; and,

a transmitter for transmitting the authorization signal;

at least a port for receiving authorization signals of the subset of 1 < N < M persons from the at least a portable biometric device; and,

a processor for determining access privileges to the secured entity or service in dependence upon the authorization signals of the subset of 1 < N < M persons.

15. A security system for securing an entity or a service from indiscriminate access as defined in claim 14, wherein the biometric sensor comprises a fingerprint imager.

16. A security system for securing an entity or a service from indiscriminate access as defined in claim 14, wherein the transmitter comprises transmission elements for wireless communication.

17. A security system for securing an entity or a service from indiscriminate access as defined in claim 14, wherein the portable biometric device comprises a handheld portable biometric device.

18. A security system for securing an entity or a service from indiscriminate access as defined in claim 17, wherein the handheld portable biometric device comprises a smart card.